UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/691,783	10/17/2000	Keith E. Moore	10003895-1	3635

7590 09/22/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/691,783	MOORE ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 0705*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-26 have been re-examined. Claims 27-31 are new claims.

2. This is a Final rejection.

Response to Arguments

3. Applicant's arguments filed July 7, 2005 have been fully considered but they are not persuasive.

Dwork discloses an encrypted authentication message and further goes into details of the decryption process of this message (col.6, lines 38-64). It is inherent encryption is based on one or more keys, hence it is also inherent that the decryption process is based on one or more keys which is the reciprocal of the encryption key.

Dwork discloses writing the encrypted information to a CD-ROM or satellite or digital cable TV (col.6, lines 25-35 and col.7, lines 25-29).

Dwork further discloses the content decryption key is obtained upon the decrypted authentication message wherein applies the authorization function to produce the authorization signal value and passes the signal to the decryption processing module whereby it is inherent that the decryption is a success that further proceed to obtain the decryption key by the module

executing the extrication function on the signet pair which yields the decryption key which is used by the decryption logic to decrypt the content (col.7, lines 54-67 and col.8, lines 18-52).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Dwork, et al. (US 6,038,316).

As per claim 1:

Dwork, et al. disclose a method for a sender to send an encrypted message to an authorized recipient, the method having steps comprising:

creating an encrypted content message that may be decrypted using a content decryption key that is unknown to the authorized recipient; **[COL.5, lines 17-21 and COL.6, lines 13-18]**

creating an encrypted authentication message that may be decrypted using a recipient's key wherein the recipient's key is known to the authorized recipient but unknown to others except perhaps known to the sender; **[COL.6, lines 38-44]**

fixing the encrypted authentication message and the encrypted content message onto a tangible medium and thereafter permitting the authorized recipient to obtain the tangible medium; **[COL.6, lines 27-37 and COL.7, lines 25-40]**

if a valid reply has been received, wherein the valid reply is based upon the decrypted authentication message, then allowing the authorized recipient to obtain said content decryption key. **[COL.6, lines 38-39 and COL.7, lines 55-56]**

As per claim 2: See col.8, lines 54-55; discussing the recipient's key is a secret key that is shared between the sender and the recipient.

As per claim 3: See col.8, line 57; discussing the recipient's key is a recipient's private key that is associated with a recipient's public key.

As per claim 4: See col.6, lines 38-39 and col.7, lines 55-56; discusses creating an encrypted authentication message further comprises a step of sender authentication encryption such that the authorized recipient may use a sender's key for decryption of the authentication message thereby authenticating that the sender was the source of the encrypted authentication message, such that the sender's key is known to the authorized recipient, and

such that the encrypted authentication message may be decrypted with a decryption step employing said recipient's key and with another decryption step employing said sender's key.

As per claim 5: See col.8, lines 54-55; discussing the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

As per claim 6: See col.8, line 57; discussing the sender's key is a public key that is associated with a sender's private key.

As per claim 7: See col.6, lines 38-39 and col.7, lines 55-56; discussing creating an encrypted content message further comprises a step of sender authentication encryption such that the authorized recipient may use a sender's key for decryption of the encrypted content message thereby authenticating that the sender was the source of the encrypted content message, such that the sender's key is known by the authorized recipient, and such that the encrypted content message may be decrypted by a decryption method with a step employing the recipient's key and with another step employing the sender's key.

As per claim 8: See col.8, lines 54-55; discussing the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

As per claim 9: See col.8, line 57; discussing the sender's key is a public key that is associated with a sender's private key.

As per claim 10:

Dwork discloses an article of manufacture for sending an encrypted message from a sender who possesses a content decryption key to a recipient who possesses a recipient's key, the article, comprising:

a tangible medium; **[COL.5, lines 21-26]**

an encrypted content message fixed on said tangible medium, wherein said encrypted content message may be decrypted using the content decryption key; **[COL.6, lines 27-37]**

an encrypted authentication message fixed on said tangible medium, wherein said encrypted authentication message may be decrypted using the recipient's key; **[COL.7, lines 25-40]**

whereby after the article is delivered to the recipient the recipient may use the recipient's key to decrypt said encrypted authentication message into a decrypted authentication message, the recipient may use the decrypted authentication message to send a valid reply to the sender confirming that the recipient received said article and the sender may then allow the recipient to obtain the content decryption key. **[COL.6, lines 38-39 and COL.7, lines 55-56]**

As per claim 11: See col.8, lines 54-55; discussing the recipient's key is a secret key that is shared between the sender and the recipient.

As per claim 12: See col.8, line 57; discussing the recipient's key is a recipient's private key that is associated with a recipient's public key.

As per claim 13: See col.6, lines 38-39 and col.7, lines 55-56; discussing encrypted authentication message is sender authentication encrypted such that said encrypted authentication message may be decrypted by a decryption method having a step employing the recipient's key and having another step employing a sender's key such that the recipient may use the sender's key to authenticate that the sender was the source of said tangible medium.

As per claim 14: See col.8, lines 54-55; discussing the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

As per claim 15: See col.8, line 57; discussing the sender's key is a public key that is associated with a sender's private key.

As per claim 16: See col.6, lines 38-39 and col.7, lines 55-56; discussing encrypted content message is sender authentication encrypted such that said encrypted content message may be decrypted by a decryption method having a step employing the recipient's key and having another step employing a sender's key such that the recipient may use the sender's key to authenticate that the sender was the source of said tangible medium.

As per claim 17: See col.8, lines 54-55; discussing the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

As per claim 18: See col.8, line 57; discussing the sender's key is a public key that is associated with a sender's private key.

As per claim 19:

Dwork, et al. a method for an authorized recipient to receive an encrypted message from a sender, the method having steps comprising:

receiving a tangible medium from the sender wherein the tangible medium has fixed upon it an encrypted authentication message and an encrypted content message; **[COL.6, lines 27-37 and COL.11, lines 42-43]**

using a recipient's key to decrypt the encrypted authentication message into a decrypted authentication message, wherein the recipient's key is known to the authorized recipient but unknown to others except perhaps known to the sender; **[COL.6, lines 38-49]**

creating a valid reply using the decrypted authentication message; sending the valid reply to the sender; **[COL.7, lines 55-56]**

if the recipient has received a content decryption key from the sender, then using the content decryption key to decrypt the encrypted content message. **[COL.7, lines 1-21]**

As per claim 20: See col.13, line 47 – col.14, line 35; discusses receiving the valid reply using the sender after permitting the authorized recipient to obtain the tangible medium, and wherein the allowing is responsive to the receiving.

As per claim 21: See col.14, lines 30-35; discussing the valid reply is generated by the recipient after the recipient obtains the tangible medium.

As per claim 22: See col.7, lines 25-57 and col.11, line 42; discusses the fixing and the allowing comprise creatings, fixing and allowing using the sender.

As per claim 23: See col.6, lines 27-37; discussing permanently fixing the encrypted authentication message and the encrypted content message onto said tangible medium.

As per claim 24: See col.6, lines 27-49; discussing the encrypted content message and the encrypted authentication message are permanently fixed onto said tangible medium.

As per claim 25: See col.5, lines 15-54; discusses the creating and the sending the valid reply comprise creating and sending using the authorized recipient.

As per claim 26: See col.7, lines 25-57 and col.11, line 42; discusses the receiving, the using, the creating, and the sending comprise receiving, the using, the creating, and the sending using the authorized recipient.

As per claim 27: See col.6, lines 25-35 and col.7, lines 25-29; discussing the fixing comprises fixing both the encrypted authentication message and the encrypted content message on to the tangible medium comprising the same medium.

As per claim 28: See col.6, lines 25-35 and col.7, lines 25-29; discussing the same medium comprises a single fixed tangible medium.

As per claim 29: See col.6, lines 25-35 and col.7, lines 25-29; discussing the single fixed tangible medium comprises a compact disc.

As per claim 30: See col.6, lines 25-35 and col.7, lines 25-29 and 54-67; discussing the recipient's key comprises using the recipient's key by the authorized recipient.

As per claim 31: See col.7, lines 54-67 and col.8, lines 18-52; discussing the Certain the valid reply comprises creating using the authorized recipient.

Conclusion

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone

number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

Primary Examiner
Art Unit 2135